Department of the Navy
Naval Information Systems
Management Center

NAVSO P-5239 -04
September 1995

INFORMATION SYSTEMS SECURITY

MANAGER (ISSM)

GUIDEBOOK

MODULE 04

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Naval Command, Control and Ocean Surveillance Center
ISE East Coast Division
Code 423
400 Marriott Drive
North Charleston, SC 29406-6504

Commercial (803) 974-6756
DSN 563-2030, extension 6756
E-Mail: subscribe@infosec.nosc.mil

Electronic versions of this document may be downloaded via anonymous ftp from infosec.nosc.mil or //http://infosec.nosc.mil/inf.html.

Stocked: Additional copies of NAVSO P-5239-04 can be obtained from the Navy Aviation Supply Office (Code 1013), 5801 Tabor Avenue, Philadelphia PA 19120-5099, through normal supply channels in accordance with NAVSUP P-600 (CD-ROM only), using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8215.

FOREWORD

The Navy Staff Office Publication (NAVSO P) 5239, *Information Systems Security (INFOSEC) Program Guidelines* is issued by the Naval Information Systems Management Center. It consists of a series of modules that provide procedure, technical, administrative, and supplemental guidance for all information systems, whether business or tactical. It applies to information systems used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data. Each module focuses on a distinct program element and describes a standard methodology for planning, implementing, and executing that element of the INFOSEC program within the Department of the Navy (DON).

This module, the *Information Systems Security Manager (ISSM) Guidebook*, describes the roles and responsibilities of the ISSM within the DON INFOSEC program.

Terminology associated with information systems in general, and INFOSEC specifically, varies from service to service and from Command to Command. The Automated Data Processing Security Officer (ADPSO) from a decade ago is now referred to as an ISSM. Section 2 discusses common DON terms for INFOSEC roles.

Organizational differences make it difficult to precisely define discrete roles and responsibilities, because organizations may choose to implement the ISSM responsibilities defined in this guidebook differently. For example, the location and size of the activity or Command, and the complexity of the ISs and networks may dictate how the role of the ISSM is implemented. In large Commands the security responsibilities defined here may be divided among numerous security personnel. Some Commands may have a single individual performing all the functions identified. Regardless of the implementation, the guidebook addresses the broadest set of functions identified for the ISSM position.

During the preparation of this guidebook, several activities were contacted and interviewed for technical inputs. The security personnel of the Commander-in-Chief, U.S. Atlantic Fleet (CINCLANTFLT), the Space and Naval Warfare Systems Command (SPAWAR), and the Naval Sea Systems Command Automated Data System Activity (SEAADSA) were extremely helpful in providing information and guidance.

TABLE OF CONTENTS

TABLE OF CONTENTS

INFORMATION SYSTEM S SECURITY MANAGER (ISSM) GUIDEBOOK

1.0 INTRODUCTION

Technological progress and growth in information systems (IS) has accelerated the expansion of information transfer, processing, and storage capabilities worldwide. Technological advances have also increased the risks associated with exploitation by both accidental exposure and malicious threat agents. Information Systems Security (INFOSEC) is the discipline that provides an integrated and systematic approach to the security of all aspects of ISs. In implementing INFOSEC, the Department of the Navy (DON) has developed several policy and procedures documents to increase personnel 's understanding and awareness of INFOSEC requirements among IS sponsors, developers, and users, and to reduce risk in ISs to acceptable levels. Navy Staff Office Publication- (NAVSO P) 5239-01, *Introduction to Information Systems Security*, further explains the implementation of INFOSEC. Definitions of terms used within this document are provided in NAVSO P-5239-02, Terms, Abbreviations, and Acronyms.

Purpose

This guidebook is a module within the NAVSO P-5239 series. This series is developed to assist in planning and operating ISs and to help system users maintain security awareness. This guidebook provides guidance and direction to current, new, and prospective ISSMs in implementing and managing overall INFOSEC programs. Specifically, it describes the responsibilities of the ISSM and provides instruction for implementing these responsibilities.

Policy and Guidance

Module NAVSO P-5239-04 was developed in accordance with Department of Defense (DOD) and DON policy. Appendix A provides a bibliography of security policy, procedure, and guidance documentation.

Document Structure

Section 2 briefly describes the ISSM's role, qualifications, prerequisites, and working relationships. Section 3 describes the ISSM's responsibilities, which are organized in 11 task areas. The first task area, Security Management, can be considered an umbrella under which the remaining 10 task areas reside. Specifically, the performance or conduct of the other 10 task areas is planned, coordinated, and facilitated under this overall management function. The 11 tasks areas are as follows:

- Security management
- Risk management program
- Accreditation
- Administrative functions
- Training and awareness
- Physical security
- Auditing
- Incident and violations reporting
- Security configuration management
- Contingency planning
- Security documentation.

2.0 INFORMATION SYSTEMS SECURITY MANAGER ROLE

The ISSM functions as the activity's focal point and principal advisor for INFOSEC matters on behalf of the Designated Approving Authority (DAA). The ISSM reports to the DAA and implements the overall INFOSEC program approved by the DAA. An activity may have multiple ISSMs. For example, an activity having several subordinate Command's may have an ISSM assigned for each subordinate Command.

The ISSM Role

In executing the responsibilities of the position, the ISSM:

- Ensures that INFOSEC program requirements are met
- Implements the risk management program required by the DON
- Verifies that appropriate security tests are conducted and documented
- Ensures that the accreditation support documentation is developed and maintained
- Provides the DAA with accreditation packages for systems under the DAA's purview to verify that each IS meets security specifications for an acceptable level of risk
- Reviews the accreditation plan and reaccreditation activities
- Ensures that proposed system changes are reviewed, and that implemented system modifications do not adversely impact the security of the system
- Ensures contingency plans are developed and tested
- Ensures that IS users' activities are monitored to verify compliance with security policies and procedures
- Coordinates regularly with Information Systems Security Officers (ISSO) and Network Security Officers (NSO), who provide system-level INFOSEC support within the confines of the ISSM's area of responsibility
- Maintains an Activity INFOSEC Plan (ISSP) and ensures the development of System Security Plans (SSP) for systems that contain sensitive information.

Qualifications/ Prerequisites

No specific formal degree program is required for the ISSM role. However, extensive experience in INFOSEC is required and a technical background in computer science, mathematics, engineering, or a related field is extremely beneficial. This

technical background must be balanced with effective management skills, because the ISSM must interact with people at all levels of the organization.

The ISSM's security education and work experience should provide familiarity with all aspects of INFOSEC, from personnel security to emanations security. Security training should include DOD and DON security courses (e.g., Navy Automated Data Processing Security Officer [ADPSO] Course, Introduction to Computer Security or equivalent courses). The ISSM should be familiar, through work experience, with the ISSO and NSO roles and responsibilities.

Relationships

In executing security responsibilities, the ISSM interacts with activities and personnel within and external to the site security organization. This section defines the roles of the activities and personnel as related to INFOSEC that directly interface with the ISSM. Some of the positions described below may not exist in all Commands. Specifically, the assignment of positions is dependent on the Command structure and is at the discretion of the DAA.

Personnel/ Activity	**INFOSEC Role**
DAA	The DAA is responsible for ensuring compliance with the DON INFOSEC Program for the activities and ISs under the DAA's jurisdiction. The DAA grants interim and final approval to operate an IS in a specific security mode based on a review of the accreditation documentation and a confirmation that the residual risk is within acceptable limits.
NSM	The Network Security Manager (NSM) acts as the focal point and principal advisor for network security matters. Depending on the size of the activity, the geographical distribution, and the complexity of the site, this role may be performed by the ISSM.

ISSO	The ISSO acts on behalf of the ISSM to ensure compliance with the INFOSEC procedures at the operational site or facility. The ISSM is responsible for performing those duties normally performed by ISSOs in the event that no ISSOs are appointed at the particular Command.
NSO	The NSO acts on behalf of the NSM or ISSM to implement the network security policy of the activity across all data networks at the activity under the NSO's authority. The ISSM is responsible for performing those duties normally performed by NSOs in the event that no NSOs are appointed at the particular Command.
Other Site Security Personnel	Other security-related billets are filled depending on the structure and size of the Command or Activity. A Site Security Manager is the principal advisor on information and personnel security in the Command and is responsible to the Commanding Officer for the management of the overall security program. Physical and Personnel Security Officers may also be designated. The ISSM is responsible to the Site Security Manager for the protection of classified information being processed on ISs. The ISSM coordinates with other security personnel to ensure the consistent implementation of security policies and procedures.
PM	The INFOSEC Program Manager (PM) is responsible for the development of a system and must be aware of the INFOSEC requirements that must be met by the specific system. After the system is fielded, the PM receives inputs on the system's operation. The PM manages the security upgrades required for the system through the In-Service Engineering Activity (ISEA) and Software Support Activity (SSA).

ISEA	The ISEA is responsible for implementing hardware (and total system) changes to the system and must coordinate with the ISSM to ensure compliance with INFOSEC policies.
SSA	The SSA is responsible for implementing software-related changes to the system, and must coordinate these changes with the ISSM to ensure no negative effect on the security posture of the IS results from a change.
System or Network Administrator	The System or Network Administrator is responsible for the administration and operation of an IS and ensures the IS operates in accordance with Command security policies and procedures. The System or Network administrator also implements changes to an IS, such as software upgrades, which are directed, in many cases, by the SSA or ISEA.
User	In this document, the term “user” refers to all personnel who access the IS for authorized purposes and in accordance with security procedures and guidelines (i.e., users, operators, and maintainers). The ISSM ensures that the IS users are aware of their security responsibilities and are trained in the user security features of the IS.

Figure 1 illustrates the relationship of the ISSM to the security roles and titles within and external to the site INFOSEC organization.

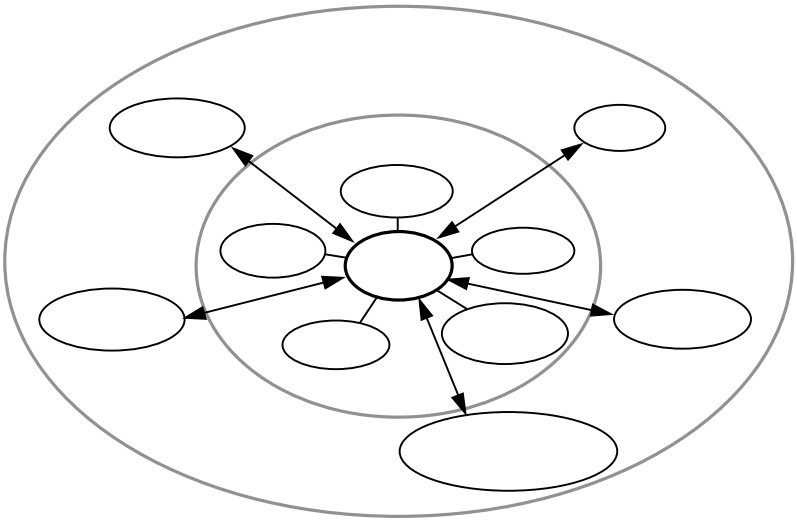

Figure 1
ISSM Internal and External Relationships

3.0 INFORMATION SYSTEMS SECURITY MANAGER RESPONSIBILITIES

The ISSM is responsible for ensuring that the INFOSEC Program requirements are met. The ISSM accomplishes this by performing, directing, coordinating, administering, and overseeing various activities and personnel. This section defines the responsibilities of the ISSM in 11 task areas.

3.1 Security Management

This section describes the responsibilities of the ISSM within the overall task area of security management, which is the umbrella covering the other 10 task areas. It specifically focuses on planning and coordinating tasks required for an effective INFOSEC program.

SECURITY POLICY AND PROCEDURES DEVELOPMENT AND APPLICATION

Responsibility

The ISSM is responsible for interpreting and tailoring DOD and DON security policy to meet the requirements of the Command or activity and ISs and networks under the ISSM's cognizance.

Implementation

Policy and Procedures Application

The ISSM remains current with all DOD and DON INFOSEC policies and procedures and is aware of changes to these policies and procedures. The ISSM ensures that all INFOSEC activity within the respective Command is in accordance with DOD and DON policy and procedures. The ISSM tailors this policy and guidance to meet the specific Command's requirements.

Key Document Development

The ISSM ensures that activity-level INFOSEC policy and guidelines are documented in an Activity ISSP in accordance with OPNAVINST 5239.1A.

The ISSM also ensures the development of SSPs for each IS that contains or processes sensitive information in accordance with OMB Bulletin No. 90-08.

Guidance

The ISSM provides guidance to subordinate INFOSEC personnel, IS users, and other personnel, as necessary, in the interpretation and implementation of the Command's INFOSEC policies and procedures.

Reference: Security policy, procedure, and guidance documentation is identified in Appendix A. Appendix A items annotated with an "*" should be maintained by every ISSM for easy reference because these documents directly pertain to the performance of the ISSM and other IS personnel roles. NAVSO P-5239-11, System Security Requirements Development, provides guidance for developing security policy and security requirements for a specific system. Also see section 3.11, Documentation, for Activity ISSP and SSP document descriptions.

INTERACTION WITH PERSONNEL

Responsibility

As the focal point for INFOSEC matters, the ISSM is cognizant of all IS-related activity and ensures that all necessary tasks and functions are adequately performed or conducted. The ISSM achieves this by conducting and attending status meetings and managing, overseeing, and coordinating efforts relative to INFOSEC. This section elaborates on the ISSM relationships identified in section 2.

Implementation

Information Systems Security Officer and Network Security Officer Appointment

The ISSM ensures that ISSOs and NSOs are appointed by the program manager of a specific branch, division, or department, as appropriate, based on the structure and needs of the specific Command or Activity. Commands having complex ISs may need more ISSOs to perform day-to-day activities and to respond to security problems and IS user needs. The following illustrates the appointment of ISSOs within different Command structures:

- Multiple ISSOs may be assigned to a single, large IS

- Site-specific ISSOs may be assigned for geographically distributed IS locations
- A single ISSO may be assigned within a Command for multiple ISs.

INFOSEC Personnel Oversight

The ISSM is responsible for overseeing ISSOs and NSOs and:

- Ensures that all IS personnel are trained in respect of functional duties and Command INFOSEC policies and procedures
- Ensures that security procedures are being followed in accordance with the Activity ISSP and that all necessary tasks are completed to maintain the security of the IS s
- Reviews and provides input to reports, checklists, Security Operating Procedures (SOP), and other documentation developed by the ISSOs and NSOs
- Provides guidance concerning the interpretation and implementation of security policies and procedures .

Reference: For more information, see section 3.5, Training and Awareness, and section 3.11, Documentation.

Coordination With Other Security Personnel

The ISSM coordinates with other security personnel within the Command (e.g., personnel, physical, industrial, and operations) to ensure that INFOSEC policies and procedures are consistent with other security department polices and procedures. For example, the ISSM works with the Physical and Personnel Security Departments to ensure the following:

- Adequate physical security safeguards are in place to protect the IS
- Terminated or transferred personnel check out with IS personnel (ISSM, ISSO, NSO, etc.) to ensure the removal of such person's system accounts on any and all ISs
- Clearance lists are up-to-date and reflect accurate clearance levels for all personnel that use the IS .

The ISSM also coordinates with the ISSM/ISSOs of Intelligence, Cryptologic, or Special Program organizations located at the

ISSM's Activity or Command. The objective of such coordination is to eliminate duplicate efforts and to standardize local procedures within the limits of need-to-know.

Liaison with Multi-Service Program Officials/ Functional Program Leads

The ISSM coordinates with Program Managers, systems engineers, ISEA and SSA representatives, and other program personnel to ensure that security issues are addressed in all phases of an IS's life cycle. At a minimum, the ISSM:

- Participates in status/management/planning meetings with cognizant activities
- Ensures that proposed changes (e.g., software, hardware components, firmware) to the IS are reviewed and that the need for reaccreditation is evaluated or considered
- Alerts cognizant program officials of security-related problems/incidents.

Reference: For more information, see section 3.3, Accreditation; section 3.9, Security Configuration Management; and section 3.8, Incident and Violations Reporting.

Liaison With System and Network Administrator(s)

The ISSM coordinates with system and network administrators, and at a minimum:

- Conducts periodic status meetings to maintain cognizance of all activities that may have an impact on INFOSEC, and to discuss problems and issues relating to security
- Reviews system changes and changes in security operating procedures, and ensures that system and network administrators implement changes correctly
- Coordinates the implementation of new security policies.

Maintain Currency With Security Services

The ISSM remains current with technological advances in INFOSEC features that can provide necessary security services. This includes, at a minimum:

- Attending security forums and working groups, such as

the DON Information Security Group
- Reviewing Government and industrial publications
- Implementing new policies, procedures, and safeguards .

The ISSM identifies and implements technological advances to enhance the security services necessary to ensure protection of the IS. Such services include:

- Denial of service protection (e.g., assuring a system has an alternate power source or assuring a system cannot be overloaded by a subversive insider or outsider who can gain unauthorized system entry)
- Integrity protection (e.g., data transfers between systems are protected by error detection correction mechanisms)
- Nonrepudiation services (e.g., establishing a third party arbitration to verify proof of origin and proof of delivery disputes)
- Confidentiality (e.g., ensuring that data is protected from browsers)
- Availability (e.g., ensuring that data and/or operating systems or software is available to authorized users)

This page left intentionally blank.

3.2 Risk Management Program

The DON Risk Management Program includes the process of identifying, measuring, and minimizing events affecting IS resources. The program includes the security activities that span the life cycle of an IS. Risk Management determines the value of the data, which protections already exist, and how much more protection (if any) the system needs. It includes risk analysis, countermeasure selections, security test and evaluation, and system review. The results of these activities provide the information on which a DAA can base an accreditation decision. Risk management activities do not end with an accreditation decision. Ongoing analysis throughout the life cycle ensures that the security requirements are always met. The ISSM implements the DON-mandated Risk Management Program for the systems under the ISSM's purview.

Responsibility

The ISSM ensures that the DON Risk Management Program requirements are met by ensuring these tasks are accomplished:

- Identify specific threats and vulnerabilities to the IS
- Identify and apply countermeasures to mitigate the identified risk
- Test the effectiveness of the implemented security controls
- Review the continued effectiveness of the implemented security measures.

Implementation

Risk Assessment

The first two tasks are accomplished by conducting a Risk Assessment. The Risk Assessment evaluates the threats and vulnerabilities related to the assets of the activity. *The Risk Assessment Guidebook*, Module 16 of the NAVSO P series, provides the procedures to be followed for performing a risk assessment based on common, definable systems or network configurations. It identifies and separates systems and networks by operating characteristics, and provides methodologies that can be used for each situation.

The ISSM is responsible for determining the risk assessment methodology to be used for each system under the ISSM's purview. The ISSM is responsible for ensuring that a risk assessment is performed on each IS under the ISSM's purview.

The ISSM is responsible for reviewing the completed Risk Assessment to ensure the following:

- The methodology was properly followed
- The risks and the risk levels were identified
- Appropriate countermeasures were identified and recommended
- Residual risk was identified.

Countermeasure Identification and Implementation

The ISSM is responsible for ensuring that threats, vulnerabilities, and current safeguards are identified in the Risk Assessment. Effective countermeasures must be identified for areas of exceptionally high or unacceptable risks.

The ISSM reviews the countermeasure selection recommendations provided with the Risk Assessment and ensures that selection of appropriate countermeasures is based on:

- The risk potential
- The magnitude of the security problem
- The potential impact on organizational resources.

The ISSM coordinates the selection of security controls with the Commanding Officer to minimize the effect of the security measures on the overall mission accomplishment.

The dynamic environment of ISs demands continuing review of the effectiveness of security controls to achieve the highest degree of protection. The effectiveness of the identified and implemented countermeasures is assessed in the Security Test and Evaluation (ST&E) performed on each IS.

Security Test and Evaluation

The primary purpose for conducting ST&E is to obtain technical information to support the DAA's decision to accredit an IS. The ST&E consists of two interrelated phases:

- Determining whether the necessary countermeasures identified in the Risk Assessment have been installed
- Determining whether the installed countermeasures are

working effectively.

The ISSM is responsible for ensuring that the ST&E requirements to support the DAA's IS accreditation decision for each Command IS processing classified or otherwise sensitive information are satisfied. This entails the following activities:

- Identifying qualified individuals to perform the ST&E activities
- Coordinating the IS Risk Assessment review to ensure the currency and accuracy of risks and identified countermeasures
- Identifying how the effectiveness of each countermeasure will be determined. Countermeasures will need to be indicated as well as the method of testing (e.g., scenarios, inspections, documentation and procedure review) to be implemented for each countermeasure
- Executing the ST&E plan and documenting the results in an ST&E report. This report should include either:
  - A recommendation to the DAA to accredit or not accredit the IS or network or grant an interim authority to operate based on the level of risk identified by the ST&E team
  - A recommendation regarding security deficiencies, if nonaccreditation is recommended.

Reference: For more information concerning ST&E documentation see section 11, Documentation. Also see NAVSO P-5239-18, *Security Test and Evaluation Guidebook*.

IS Modifications

The IS environment requires constant review to ensure the security features are providing the required protection. Changes to any IS affect security. Changes to security can affect the accreditation status of the IS.

The ISSM ensures the review of any planned changes or modifications to the IS to assess the impact to the overall security of the system. Types of changes that can affect security include, but are not limited to:

- Changes in the level and type of data being processed
- Redesigns of the application software

- Revisions or new releases of the operating system
- Changes in the hardware

- Upgrades in the central computer facility
- Security violations revealing a security design flaw
- New threats and vulnerabilities discovered through community awareness mechanisms.

The ISSM makes recommendations to the DAA regarding the need to initiate reaccreditation activities as a result of any change to the overall security of the IS.

Reference: For more information concerning the ISSM's role regarding security configuration management (CM), see section 3.9, Security Configuration Management.

3.3 Accreditation

Accreditation is the DAA's formal process and declaration that security countermeasures have been properly implemented for the activity's IS or networks consistent with protection requirements, and that the applicable steps of the accreditation process have been accomplished. The DAA bases the accreditation decision on a review of the accreditation support documentation. This documentation consists of:

- Activity ISSP
- Risk assessment
- ST&E documentation
- Accreditation recommendation
- Contingency plan.

The DAA either concurs with the information presented, declaring that a satisfactory level of operational security is present, or does not concur, indicating that the level of risk has not been adequately defined or has not been reduced to an acceptable level for operational requirements.

If accreditation is not granted, the IS may operate if the DAA issues an "interim authority to operate." Interim authority to operate is granted for a fixed period of time, generally a year. This authority is based on an approved Activity ISSP, and is contingent on identified conditions being met. The interim authority to operate, while continuing the accreditation process, permits the activity to meet its operational mission requirements while improving its INFOSEC posture. Interim authority to operate is not a waiver of the requirement for accreditation.

Responsibility	The ISSM ensures that all activities required to accredit and reaccredit an IS are completed.
Implementation	The ISSM develops and maintains the IS activity accreditation schedule (AAS), an attachment to the Activity ISSP. In addition to identifying the DAA and providing relevant IS information, the schedule provides: · Risk assessment development dates · ST&E plan development and test dates · Contingency plan development dates. The ISSM is responsible for reviewing the accreditation documentation before submitting it to the DAA for action. The ISSM will review the documentation to ensure that it

substantiates

the accreditation recommendation. The ISSM will ensure that the residual risk identified in the Risk Assessment is clearly presented to the DAA. The ISSM will ensure that the results of the ST&E clearly reflect the security posture of the IS. The ISSM will ensure that the DAA is aware of all risks associated with operating the IS in a particular mode using a prescribed set of safeguards. In some instances, for noncritical systems, approval authorization can be delegated directly to the ISSM.

Reference: For more information concerning the AAS and ST&E documentation, see section 3.11, Documentation. For more information concerning Contingency Plan development, see section 3.10, Contingency Planning. NAVSO P-5239-13, the
Certification and Accreditation (C&A) Guidebook, provides procedure guidance and decision aids for conducting C&A activities.

3.4 Administrative Functions

The appointed ISSOs/NSOs perform the day-to-day security administrative tasks associated with the IS. The ISSM provides oversight and guidance to these functions as required for successful implementation of the Command's INFOSEC policies and procedures, as documented in the Activity ISSP. Additional information concerning the performance of these tasks is provided in NAVSO P-5239-07 (the *Information Systems Security Officer Guidebook*) and NAVSO P-5239-08 (the *Network Security Officer Guidebook*).

Responsibility

The ISSM oversees and provides guidance to ISSOs and NSOs for the performance of the administrative tasks that follow.

Implementation

Accounts Administration Oversight

The ISSM provides oversight to the ISSO/NSO in accounts administrative tasks. These tasks include:

- User Accounts
  - Ensuring that users hold proper clearances
  - Working with the Command's personnel security department to ensure that an accurate and up-to-date record of personnel clearances is maintained
  - Ensuring that users are trained in applicable security requirements and responsibilities.
- Account Terminations
  - Coordinating with the Command's physical and personnel security departments to delete users from physical and IS authorization access lists
  - Coordinating with the Command's physical and personnel security departments to ensure that all physical access materials, (e.g., tokens and cards), are returned by user
  - Coordinating with the Command's physical security department to ensure that locks are changed each time a user leaves, and on a routine basis in accordance with the Command's security policies
  - Coordinating with the system/network administrator to ensure that the user's data within an account is disposed of properly and that the account is closed.

Reference: For more information, see section 3.5, Training and Awareness, and section 3.6, Physical Security.

IS Media Administration Oversight

The ISSM provides oversight to the ISSO/NSO in IS media (hardware, software [applications and work files], and firmware) administrative tasks, such as:

- Ensuring that users are educated in the Command's policies and procedures for marking, handling, and accounting for IS hardware, software, and firmware
- Coordinating with the system and network administrators for maintaining an inventory of the IS components and the other cognizant security departments (e.g., document control, physical) for handling and marking classified components and software. The ISSM and subordinate security officers should exploit plant property inventories (maintained by activity property management staff), to the maximum extent possible.
- Ensuring that Command policies and procedures are incorporated in declassification and downgrading procedures and coordinating with the system and network administrators and cognizant security department (document/media control) to:
  - Develop/implement purging, declassifying, and downgrading procedures
  - Acquire, as necessary, special hardware (e.g., degaussers) for sanitizing systems.
- Ensuring that users and system and network administrators implement Command policies and procedures when destroying or disposing of IS media resources.

Reference: For more information concerning classifying and safeguarding classified information (e.g., marking and handling of media resources, declassification/downgrading and upgrading of classified components, destruction of classified material) see OPNAVINST 5510.1H and NAVSO P-5239-26, *Remanence Security Guidebook*.

Virus Control and Reporting Program Oversight

The ISSM provides oversight and guidance to the ISSO and NSO in implementing a virus control and reporting program that ensures proper measures are taken to protect the IS from computer viruses. The ISSM reports all virus attacks to the Naval Computer Incident Response Team (NAVCIRT) and ensures that the ISSO and NSO:

- Implement training programs to educate users in the dangers of computer viruses, virus protection methods, and virus reporting procedures
- Work with system administrators to implement procedures for reporting actual or suspected viruses
- Work with system administrators to choose and acquire suitable software to protect the IS against viruses.

Reference: For more information, see section 3.8, Incident and Violation Reporting. Also see NAVSO P-5239-19, *Computer Incident Response Guidebook*.

Security "Watchdog" Oversight

The ISSM provides oversight and guidance to the ISSO and NSO in implementing the security "watchdog" role. Specifically, this function (performed by the ISSO and NSO) includes monitoring system use and conducting random floor and system component checks to ensure compliance with Command INFOSEC policies and procedures.

Reference: For more information concerning floor checks see NAVSO P-5239-07, the *Information Systems Security Officer Guidebook*, or NAVSO P-5239-08, the *Network Security Officer Guidebook*.

This page left intentionally blank.

3.5 Training and Awareness

The ISSM is responsible for developing security training. This training will include training for INFOSEC personnel, training for IS users, and fostering INFOSEC awareness. The ISSM plans and develops Command and IS-specific training based on the security policies and procedures documented in the Activity ISSP. The ISSM ensures that all new personnel are trained shortly after induction and that refresher training is provided periodically to all personnel.

Responsibility

The ISSM is responsible for developing two types of security training: training for INFOSEC personnel (ISSOs and NSOs) and training for IS users. The ISSM is also responsible for fostering IS user security awareness.

Implementation

INFOSEC Personnel Training

Training for ISSOs and NSOs addresses all task areas required of the specific position.

- Format: The format for training INFOSEC personnel depends on the Command structure and number of security personnel, as described below:
  - For large Commands with many ISSOs/NSOs, formal training sessions, using a brief-style format with hands-on demonstrations is beneficial
  - For small Commands having only one or two ISSOs/NSOs, informal or on-the-job training, using handbooks and/or handouts may be desired.

When using either format, the ISSM should provide written guidelines of the responsibilities of the ISSO/NSO tailored for the specific IS. Softcopy of documents on removable computer media can be a cost effective substitute for hard copy versions.

- Curriculum: Training curriculum should include the following:
  - Instruction for the performance of all Command-specific INFOSEC procedures and duties
  - Samples of documentation to be developed by the ISSO/NSO, as required by the specific Command, such as:

- Security Operating Procedures
- Risk Assessments
- Test Plans, Procedures, and Reports
- Security Checklists
- User Warning Messages
- Authorized User Lists

- Command- and IS-specific security procedures and features, as documented in the Activity ISSP and SSPs.

The ISSM ensures that all INFOSEC personnel (including the ISSM) attend DOD- and DON-level security training, such as the DON Introduction to Computer Security Program Course offered by the Naval Computer and Telecommunications Command, the DOD Computer Institute Information Resource Protection Course, and National Institute of Standards and Technology/National Computer Security Center National Information System Security Conferences.

IS User Security Training

In accordance with the Computer Security Act of 1987, the ISSM is responsible for ensuring that all IS personnel who work with or in the vicinity of the IS receive INFOSEC training. The ISSOs/NSOs may assist in the development of training curriculum
and may conduct training sessions under the guidance of the ISSM.

- Format: The ISSM develops formal training sessions using a brief-style format with hands-on demonstrations. Written guidelines, handbooks, or hard copies of the brief should be provided to and retained by attendees for reference purposes. Softcopy of documents on removable computer media can be a cost effective substitute for hard copy versions.
- Curriculum: The training curriculum should be tailored to the specific Command and IS, and should include:
  - Value of computer-based information
  - Computer vulnerabilities
  - Basic safe computing
  - Password management
  - Virus prevention and detection
  - Command-specific security procedures

- Explanation and demonstration of security mechanisms and safeguards on the IS

- Importance of self-monitoring (e.g., identify successful and unsuccessful logons to aid in monitoring attempts by unauthorized personnel to access the system)
- Importance of being alert to suspicious/unusual activity.

Reference: For more information concerning user training course content see NAVSO P-5239-07, the *Information Systems Security Officer Guidebook*, or NAVSO P-5239-08, the *Network Security Officer Guidebook*.

Security Awareness

The ISSM ensures that user interest and awareness of security issues and procedures is maintained. ISSOs and NSOs assist in fostering user awareness. The following approaches heighten user security awareness:

- Developing and distributing security awareness posters
- Displaying warning messages on the IS (e.g., to flash when user logs on)
- Disseminating new security information and security reminders through memos, newsletters, and automated bulletin boards
- Providing hands-on demonstrations of INFOSEC features and procedures.

This page left intentionally blank.

3.6 Physical Security

Physical Security is the protection and preservation of informational, physical, and human assets through the reduction of exposure to various threats that can produce a disruption or denial of IS services or unauthorized disclosure. These measures include protections against loss or damage from:

- Intruders
- Vandals
- Environmental hazards (fire, flood/water, extreme temperature, etc.)
- Accidents.

Measures implemented depend on the site-specific environment and the classification level of the data being handled by the IS.

Responsibility

The total protection of the IS requires the ISSM to perform security activities across the wide range of security areas. Reducing the threats to an IS requires physical protection of the assets. The ISSM coordinates physical access, facility access, and environmental controls. This section describes the ISSM's roles and responsibilities in the physical protection of IS assets. The ISSM may delegate these responsibilities to the ISSO or NSO, as appropriate, depending on the Command structure.

Implementation

Facility Access

The ISSM ensures that ISSOs and NSOs coordinate with the physical security department to ensure the necessary physical safeguards are in place to protect the IS, such as:

- Locks, bars, and other physical safeguards (to include the routine changing of locks and combinations in accordance with Command policies and security operating procedures)
- Guard areas and security checkpoints
- Clearly marked security areas (with posters, signs, and warning markers)
- Intrusion detection systems (including motion sensors and video cameras)
- Alarms, signals, and reports.

User Identification and Authentication

The ISSM provides oversight and guidance to the ISSO and NSO in implementing Command policies and procedures for IS user identification and authentication, including the following:

- Ensuring that identification/authentication data bases are accessible by INFOSEC personnel only
- Providing guidance to users for developing and using unique passwords
- Working with system and network administrators to ensure that only authorized personnel (i.e., ISSO, system and network administrators) have access to and are able to execute system utilities (to prevent intentional or unintentional damage to the IS)
- Working with the personnel security department to maintain an accurate list of authorized IS users, including contractors and visitors.

Data Access

The ISSM provides oversight and guidance to the ISSO and NSO in implementing measures to prevent disclosure of information to unauthorized individuals. Such measures include:

- Ensuring that site-specific Discretionary Access Controls (DAC) and Mandatory Access Controls (MAC) policies are defined and implemented
- Controlling access to all functions that affect security or integrity of the system
- Ensuring that access control mechanisms/software are installed and operated in a manner that supports the INFOSEC policy.

Reference: For more information concerning Controlled Access Protection (CAP), see NAVSO P-5239-15, *Controlled Access Protection Guide*.

Environmental Hazards Protection

The ISSM ensures that ISSOs and NSOs coordinate with the physical security or site maintenance departments to ensure environmental controls are in place relative to the IS, including:

- Fire prevention (e.g., alarms, sprinklers, and extinguishers)
- Temperature/humidity controls

- Evacuation procedures

- Safety (warning labels, markings, signs)
- Filtered power
- Power grounding
- Flood measures
- Earthquake measures.

TEMPEST

The ISSM is responsible for coordinating with appropriate personnel (e.g., technical program activities/engineers) to ensure that TEMPEST Program requirements are met, if applicable.

This page left intentionally blank.

3.7 Auditing

Security-related weaknesses of the IS must be identified and eliminated. Monitoring the security activities of the IS and conducting an audit of security-related activity on the IS helps identify the weaknesses. This section describes the ISSM's roles in monitoring security activities on the IS.

Responsibility

The ISSM is responsible for ensuring that IS transactions are effectively audited and that audit trails are regularly reviewed by the ISSO or NSO responsible for the IS or network under the cognizance of the ISSM.

Implementation

Audit Procedures

Auditing allows the ISSM to monitor security-related activities on the IS and to evaluate risks and vulnerabilities. The ISSM ensures that:

- Appropriate security events to be audited are selected
- A reasonable and appropriate audit schedule is maintained
- Audit activities do not adversely affect IS functions
- Audit activities comply with other site-specific security procedures and requirements
- All occurrences of warning messages are investigated
- Audit trail data is protected.

Audit Trail

The audit trail is the product of audit activities. It provides a record of all security-related activities (e.g., access of classified information, logons, and logoffs). The ISSM reviews audit trails
on a periodic basis. These reviews focus on:

- Identifying streamlined methods for collecting audit information
- Ensuring that audit trail reviews by the ISSOs are used to develop accurate IS use patterns and user access reports.

This page left intentionally blank.

3.8 Incident and Violations Reporting

Security incidents or violations are occurrences that may affect the security posture of the IS. Security incidents or violations include the following:

- Suspected or confirmed viral infection
- Intrusion attempts and successes within the IS, such as:
  - Remote users logging in with compromised passwords
  - Compromised administrative privileges, allowing the creation of and use of false user accounts.
- Access denials, such as:
  - Incorrect password violations
  - Incorrect account/user names
  - Unauthorized access to certain files, directories, servers, or other resources on the IS.

Responsibility

All suspected incidents or violations must be reported immediately, first by the ISSO to the ISSM, and then after analysis by the ISSM, to the NAVCIRT and the DAA. The ISSM is responsible for approving the incident reporting mechanism.

Implementation

Incident Reporting Mechanism

The ISSM ensures that the mechanism facilitates the reporting of:

- All access denials, repeated failed logon attempts, and other unusual activities
- Viruses or suspected viruses and the forwarding of all virus reports to NAVCIRT
- All intrusion attempts/successes.

The ISSM ensures that the incident reporting mechanism meets Command and INFOSEC requirements. The mechanism should include the following, at a minimum:

- Warning message and warning report monitoring
- Access denial proceedings
- Security problem analysis
- Investigation of actual or suspected compromise of

classified information
- Virus reporting.

The ISSM participates in the preparation of the security reporting mechanism through the following actions:

- Prepares inputs to Security Operating Procedures
- Reviews and approves the procedures for reporting, investigating, and resolving security incidents
- Reviews reports of security incidents.

Incident Analysis

The ISSM must be aware of all security incidents and violations. The ISSM participates in the incident analysis through the following actions:

- Analyzes the effects of an incident as to risk and degree of compromise
- Reports results of analysis to the DAA
- Recommends appropriate action to the DAA, such as:
  - Termination of user privileges
  - Increasing auditing activity
  - Increasing protection levels and security mechanisms
  - Suspension of all noncritical IS activity
  - Complete system shutdown.

Security Vulnerabilities and Problems

The ISSM participates in the continuous assessment of the security features of the IS. With respect to security incident and violations reporting, the ISSM periodically assesses possible areas of security weakness within the IS, and viable security threat prevention measures.

Reference: See section 3.11, Documentation, for a description of an incident report and NAVSO P-5239-19, *Computer Incident Response Guidebook*.

3.9 Security Configuration Management

After security is established for an IS, strict measures must be enforced to ensure that changes to the IS do not disrupt this balance. Even seemingly minor changes may result in severe implications to the security of the system. Configuration management controls changes to system software, firmware, hardware, and documentation throughout the life of the IS. This includes the design, development, testing, distribution, and operation of modifications and enhancements to the existing IS.

Responsibility

In accordance with the DAA's policies and procedures for controlling changes to the IS, the ISSM provides input to IS configuration management activities to ensure that implemented changes do not compromise the security of the system. In this capacity, the ISSM provides security oversight, guidance, and input to system and network administrators, SSAs, ISEAs, and other activities responsible for implementing changes to the IS. The ISSM may delegate security-related configuration management activities to ISSOs or NSOs as appropriate for the specific Command.

Implementation

The ISSM is responsible for ensuring that the following tasks are conducted:

- IS inventory is reviewed regularly. Although the system or network administrator usually develops and maintains the inventory of the IS, the ISSM must closely monitor this effort to ensure that system components have not changed, been moved, or otherwise been tampered with in any way that may impact the overall security of the IS
- Documentation detailing the IS hardware, software, and firmware configuration and security features is maintained
- IS change proposals are reviewed according to the following criteria:
  - How will the change impact the security of the IS?
  - If new software is proposed, is it from an authorized source?
  - Have security features and mechanisms been considered and included in system change plans?
  - Do system support personnel know how to install and maintain new security features/mechanisms?
  - Will reaccreditation be necessary?

- Implemented changes are thoroughly tested to ensure that:
  - Changes do not adversely impact the security of the system
  - Security features and mechanisms are fully functional .

Reference: For more information concerning the types of changes that may affect security, see section 3.2, Risk Management, under IS Modifications.

3.10 Contingency Planning

By formulating plans to respond to an unplanned disruption of service to the IS or network, the ISSM will measure potential impact of incidents, accidents, or disasters on the accomplishment of the mission. This section defines the ISSM's role in preparing for an unplanned disruption of service to the IS or network.

Responsibility

The ISSM is responsible for ensuring the development and testing of contingency plans that accommodate all activity ISs for which unplanned disruption of service would have a critical impact on mission accomplishment. If the unplanned disruption of service would not have a critical impact on mission accomplishment, the ISSM informs the DAA, and no contingency plan is required. When a contingency plan is required, the ISSM ensures the annual testing and evaluation of each specific plan.

The activity's environment, the criticality of the functional applications supported by the IS, and the user's support requirements influence the scope and depth of the contingency plan. The contingency plan identifies the actions required if the normal IS environment is impaired or disrupted. The disruption can range from a few minutes to a few days depending on the cause or situation. The contingency plan addresses this entire range as it applies to the activity's IS environment. Therefore, the contingency plan should address these three situations:

- Limited loss of IS capability
- Interruption to operations
- Major damage or destruction of the facility.

Implementation

The ISSM ensures the performance of tasks associated with the development of a contingency plan:

- Assigns planning responsibility
- Establishes the contingency plan team
- Reviews the risk assessment
- Identifies emergency response planning activities
- Identifies backup operations planning requirements
- Determines recovery planning needs
- Provides education and training

- Develops plans for emergency destruction of classified data
- Establishes procedures for implementing the contingency plan
- Tests the contingency plan.

The ISSM ensures the revision of the contingency plans as necessary.

Reference: For more information concerning the development of Contingency Plans, see Federal Information Processing Standards (FIPS) Publication # 87, dated 27 March 1981.

3.11 Security Documentation

The following documentation, appearing in the order that they are referenced in this document, are typically prepared by INFOSEC personnel.

Activity INFOSEC Plan (ISSP)

The Activity ISSP is a Command-level document for implementing the security policies set forth in OPNAVINST 5239.1A. The Activity ISSP establishes local security policies, defines security scope and objectives, and assigns responsibilities at the local activity level to conduct the provisions of OPNAVINST 5239.1A. The Activity ISSP addresses both the short range and long range security goals of the activity. The plan documents the current INFOSEC environment, establishes program objectives, and outlines a Plan of Action and Milestones (POA&M) for program implementation. It references other more detailed documents such as contingency plans, risk assessments, audit trails, and test documentation. This enables the plan to be used as an effective management tool without requiring repetition of existing documentation. The Activity ISSP should be a living document to be used by the activity for baselining, updating, improving, developing, maintaining, and managing INFOSEC requirements. In accordance with OPNAVINST 5239.1A, the plan should cover the following areas:

- Scope
- Commanding officer's policy statement
- INFOSEC organization and assignment of responsibilities
- Objectives for implementing the activity INFOSEC program
- Description of the current INFOSEC environment
- INFOSEC training
- Audit/internal review
- Security in Life Cycle Management
- INFOSEC hardware/software configuration control
- Activity accreditation schedule.

System Security Plan

The SSP fulfills the Computer Security Act of 1987 that requires Federal agencies to identify each computer system that contains sensitive information and to prepare and implement a plan for the security and privacy of

these systems. The SSP, in accordance with OMB Bulletin No.

90-08, provides a basic overview of the security and privacy requirements of the specific system(s) and the Command's plan for meeting those requirements. Each SSP should include the following basic sections:

- System identification
- Sensitivity of information
- System security measures
- Additional comments.

Risk Assessment

A Risk Assessment identifies the threats, vulnerabilities, and risks to an IS. The NAVSO P-5239-16, the Risk Assessment Guidebook, presents a methodology for conducting a risk assessment using one of four types: survey, basic, intermediate, and full risk assessment.

ST&E Documentation

The following documentation are typically developed as part of the ST&E effort.

Plan and Procedures

The ST&E plans and procedures identify each of the countermeasures to be tested and the method used to determine the effectiveness of the countermeasure. If scenarios, inspections, documentation, and review procedures are to be used, they must be linked with each countermeasure.

Checklist

ST&E checklists can be used to evaluate the effectiveness of countermeasures implemented on an IS. The checklist approach may be appropriate when a full-blown ST&E is deemed unnecessary by the DAA, as determined by the complexity of the IS and the level of risk. The checklists help ensure that the IS is operating within an acceptable level of risk.

Report

The ST&E report documents the execution and results of the ST&E plan/procedures. It analyzes the findings of the ST&E plan/procedures and lists the recommendations to correct any identified deficiencies.

Activity Accreditation Schedule (AAS)	Included in the ISSP, the AAS identifies all IS elements and provides a POA&M for completing the following: · Risk assessments · Security test and evaluations · Contingency plans.
IS Incident Report	The IS incident report explains of the type of incident, the individuals involved, the estimated cost of the incident, summarizes the incident, and the investigation results along with the supervisor's recommendations; and provides the local action to prevent reoccurrence.
Authorized User List	The ISSO and cognizant local work area security officer must be able to determine the identity of all users approved for any workstation or terminal. The exact method and format can vary. Timeliness and accuracy are most important. The Authorized User List identifies authorized system users and should be kept as part of the related accreditation documentation.
Security Operating Procedures	OPNAVINST 5239.1A requires that security procedures be developed, documented, and presented to all users of ISs. Topics of discussion should include, but are not limited to: policy statement, system access controls, operating procedures, audit trails, training, physical security, media protection, modes of operation, emergency procedures, enforcement, documentation, data levels, etc. Additional information may need to be addressed to meet site-specific needs. The ISSO is the primary author of the SOPs. The ISSM ensures that SOPs are reviewed annually for accuracy.
Training and Awareness Documentation	The purpose of training and awareness documentation is to continuously reinforce the need for security of the IS and network with the users. The reinforcement satisfies the requirement to provide refresher training to the user. An awareness program provides the opportunity to

update the

user on any security changes. The program can consist of posters, newsletters, videos, warning messages, etc., to reinforce the need for protection.

Contingency Plan

The Contingency Plan provides a decision-making process to be used during or following the occurrence of unforeseen events that adversely affect normal IS operations within the activity. Activities develop a Contingency Plan that accommodates all activity ISs for which unplanned disruption of service would have a critical impact on mission accomplishment. A Contingency Plan is not required for ISs or components for which the unplanned disruption of service would not have a critical impact of mission accomplishment. In these cases the ISSM informs the DAA that no Contingency Plan is required. Mission criticality of the system determines details of Contingency Plan.

APPENDIX A

SECURITY POLICY, PROCEDURE, AND GUIDANCE DOCUMENTATION

Security Policy , Procedure, and Guidance Documentation

Items marked with an asterisk should be maintained by every ISSM for easy reference.

Department of Defense (DOD)

Department of Defense Instruction 5000.2 , Defense Acquisition Management Policies and Procedures, 23 February 1991.

This document establishes an integrated framework for translating broadly stated mission needs into stable, affordable acquisition programs that meet the operational user's needs and can be sustained, given projected resource constraints. It also establishes a rigorous, event-oriented management process for acquiring quality products that emphasizes acquisition planning, improved communications with users, and aggressive risk management by both Government and industry.

***Department of Defense Directive 5200.1** , Information Security Program, 7 June 1986.

This document reissues DOD 52001-R, "Information Security Program Regulation", updates policies and procedures of the DOD Information Security Program, implements DOD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," delegates authority, and assigns responsibilities.

***Department of Defense Regulation 5200.1-R** , Information Security Program Regulation, Department of Defense, August 1982.

This document governs the DOD information security program. It establishes a system for the classification, downgrading, and declassification of classified and sensitive information. It further states the policies and procedure s for safeguarding national security information from unauthorized disclosure.

Department of Defense Directive C-5200.5 , Communication Security (COMSEC) (U), Confidential, 21 April 1990.

This document presents the policy necessary to ensure the security and protection of telecommunications systems that transmit classified and sensitive information. This information is highly susceptible to interception, technical exploitation, the human intelligence (HUMINT) threat, and other dimensions of the foreign intelligence threat.

Department of Defense Directive C-5200.19 , Control of Compromising Emanations (U), Confidential, 23 February 1990.

***Department of Defense Directive 5200.28,** Security Requirements for Automated Information Systems, Department of Defense, March 1988.

This document provides the mandatory, minimum Information Security (INFOSEC) requirements for processing classified, sensitive unclassified, and unclassified information. The directive states that information in ISs shall be safeguarded at all times by computer, communication, administrative, personnel, operations, emanations, and physical security measures. It emphasizes the importance of a life cycle management approach for implementing computer security requirements.

***Department of Defense Directive 5200.28-STD** , Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense, December 1985.

This document is also known as the "Orange Book" and "the Criteria," this directive provides technical security requirements and evaluation methodologies for trusted computer systems. It provides a metric with which to evaluate the degree of trust that can be placed in a computer system. This standard also serves as a basis for specifying security requirements in computer system acquisition documentation.

Department of Defense Instruction 5215.2 , Computer Security Technical Vulnerability Reporting Program (CSTVRP), 2 September 1986.

This document establishes 1) CSTVRP under the direction of the National Security Agency, National Information Security Assessment Center (NISAC), 2) procedures for reporting all demonstrable and repeatable technical vulnerabilities of Automated Information Systems (IS), 3) procedures for the collection, consolidation, analysis, reporting or notification of generic technical vulnerabilities and corrective measures in support of the DOD Computer Security requirements and 4) methodologies for dissemination of vulnerability information.

Department of the Navy

SECNAV 5200.32A , Acquisition Management Policies and Procedures for Computer Resources, 03 May 1993.

This document provides policy for acquiring Department of the Navy (DON) computer resources and establishing the internal management processes. It authorizes the promulgation of the Open System Interface Standards List (OSISL) and the Products Accepted List (PAL) in SECNAVNOTE 5200, Subj: Acquisition Management Policies and Procedures for Computer Resources, to facilitate the acquisition of computer resources in accordance with this instruction.

SECNAVINST 5231.1C , Life Cycle Management of Automated Information Systems within the Department of the Navy, 10 July 1992

This document updates policy relative to Life Cycle Management (LCM) as the standard discipline for managing and obtaining approval for Information Systems (IS) projects as defined by Department of Defense Directive (DODD) 7920.1 "Life Cycle Management of Automated Information Systems (NOTAL)," 20 June 1988 and DODI 7920, "Automated Information System Life Cycle Management Review and Milestone Approval Procedures (NOTAL)," 7 March 1990.

***SECNAVINST 5239 .3**, Department of the Navy Information Systems Security (INFOSEC) Program, Department of the Navy, July 1995.

This document establishes the DON INFOSEC program within the Information Warfare discipline. It defines the organizational responsibilities for implementing the security disciplines of Communications Security (COMSEC), Computer Security (COMPUSEC), and Emanations Security (TEMPEST). This instruction provides the basic policy and guidelines necessary for consistent and effective application of resources in ensuring the security of national security systems and the security and privacy of DON systems/information under the Computer Security Act of 1987.

***OPNAVINST 5239.1A** , Department of the Navy Automated Data Processing Security Program, Department of the Navy, August 1982.

This document consolidates Navy policies on the security evaluation of ISs. The instruction delineates the requirements and assigns roles and responsibilities for accreditation of ISs. It provides guidance for the risk assessment process and full accreditation requirements.

OPNAVINST 5510.1H , Guidance for Marking and Handling Classified Material, 29 April 1988.

This document provides guidance for classifying and safeguarding classified information.

Marine Corps Order P5510.14 , Marine Corps Automatic Data Processing (ADP) Security Manual, 2 January 1981.

This document provides centralized guidance and uniform policy on all known and recognized aspects of ADP security. It also provides realistic guidance and generalized procedures to ensure that all sensitive defense information handled by automated systems is protected against espionage, sabotage, fraud, misappropriation, misuse, or inadvertent or deliberate compromise.

Marine Corps Order 5271.1 , Information Resources Management (IRM) Standards and Guidelines Program, 10 June 1993.

This document establishes the IRM Standards and Guidelines Program and authorizes the development and distribution of publications. The IRM Program is the primary means through which technical direction is exercised. The program is designed to facilitate the rapid publication of standards and guidelines covering all aspects of the management of information resources, including INFOSEC.

Executive Office/Congress and National Branch

Executive Order 12 958, Classified National Security Information, 17 April 1995.

This document established a system for classifying, declassifying, and safeguarding national security information. It identifies classification authorities and describes their general responsibilities for the origination and handling of classified information.

National Security Decision 42 , National Policy for the Security of National Security Telecommunications and Information Systems, Executive Office of the President, July 1990.

This document establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation.

National Telecommunications and Information Systems Security Policy No. 200 , National Policy on Controlled Access Protection, National Telecommunications and Information Systems Security Committee, July 1987.

This document, under the authority of NSDD 145, National Telecommunications and Information Systems Security Policy (NTISSP) No. 200 , defines the minimum level of protection for ISs processing classified or sensitive unclassified information. It prescribes the C2 class criteria of DOD 5200.28-STD as the minimum level of protection for such systems, with additional protection required if warranted by a system risk assessment.

Public Law 100-235 , Computer Security Act of 1987, 8 January 1988.

This document redefines the role of the National Institute of Standards and Technology (formerly the National Bureau of Standards) and establishes a new Computer System Security and Privacy Advisory Board. It requires each federal agency to provide for mandatory periodic training in computer security awareness and accepted computer security practices; identify each federal computer system and system under development that contains sensitive information; establish a plan for security and privacy of such systems.

Joint Staff

Chairman of the Joint Chiefs of Staff Instruction CJCSI 6510.01 , Joint and Combined Communications Security, 1 September 1993.

This document establishes policy and procedures for planning and conducting joint and combined COMSEC, and presents the following applicable policy to joint and combined applications: Transmission of Sensitive Information, System Planning, Operational Planning, Joint Coordination, Urgent Need, Foreign Release, Foreign Sales, Radios, Special-Purpose Cryptographic equipment, Manual Systems Cryptonet Size, Cryptoperiod, Radio Frequencies, Call Signs, Field Generation and Over-The Air Distribution (OTAD) of Tactical Key, Intertheater COMSEC Package Key, Assessments, COMSEC Monitoring and TEMPEST.

JCS Memorandum MJCS-38-89 , Use of Standard Embedded Cryptography, 2 March 1989.

This document encourages maximum use of standard embedded cryptography products in future communications and computer systems that require cryptographic security features.

National Computer Security Center

***CSC-STD-002-85**, Department of Defense Password Management Guideline, 12 April 1985.

This document assists in providing credibility of user identity by presenting a set of good practices related to the design, implementation, and use of password-based user authentication mechanisms. It is intended that the features and practices described in the guideline be incorporated into DOD ADP systems for processing classified or other sensitive information.

***CSC-STD-003-85**, Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, National Computer Security Center, June 1985.

This document provides guidance for specifying computer security requirements for the DOD by identifying the minimum class of system required for a given risk index.

***CSC-STD-004-85**, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in specific Environments, National Computer Security Center, June 1985.

This document provides background discussion and rationale for CSC-STD-003-85, and provides additional and more detailed guidance for specifying computer security requirements for the DOD by identifying the minimum class of system required for a given risk index for different environments.

***CSC-STD-005**, Department of Defense Magnetic Remanence Security Guideline, 15 November 1985.

This document provides procedures and guidelines for declassifying and clearing ADP magnetic memory and other ADP magnetic storage media.

NCSC-TG-001, A Guide to Understanding Audit in Trusted Systems, Version 2, 1 June 1988.

This document provides a set of good practices related to the use of auditing in automatic data processing systems employed for processing classified and other sensitive information.

***NCSC-TG-003**, A Guide To Understanding Discretionary Access Control In Trusted Systems, Version 1, 30 September 1987.

This document discusses issues involved in designing, implementing, and evaluating DAC mechanisms. Its primary purpose is to provide guidance to manufacturers on how to select and build effective DAC mechanisms.

NCSC-TG-005, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, Version 1 , July 1987.

The TNI or "Red" Book" was issued by the National Computer Security Center (NCSC) as part of its program to promulgate technical computer security guidelines. The interpretation extends the evaluation classes of the "Orange Book" to trusted network systems and components.

NCSC-TG-017, A Guide To Understanding Identification And Authentication In Trusted Systems, Version 1, September 1991.

This document provides guidance to vendors on how to design and incorporate effective identification and authentication (I&A) mechanisms into their systems. It also aids vendors and evaluators in understanding I&A requirements.

***NCSC-TG-027**, A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems, National Computer Security Center, Version 1, May 1992.

This document helps ISSOs understand their responsibilities for implementing and maintaining security in a system. This guideline also discusses the roles and responsibilities of other individuals who are responsible for security and their relationship to the ISSO, as defined in various component regulation and standards.

NCSC-TG-028, Assessing Controlled Access Protection, Version 1, 25 May 1992.

This document explains the controlled access protection requirements of the Trusted Computer System Evaluation Criteria.

NCSC-TG-029, Introduction to Certification and Accreditation, Version 1, January 1994.

This document provides an introduction to C&A concepts, provides an introductory discussion of some basic concepts related to C&A, and sets the baseline for further documents.

National Institute of Standards and Technology

***Federal Information Processing Standard s Publication 87**, Guidelines for Contingency Planning, 27 March 1981.

This document provides guidelines to be used in the preparation of IS contingency plans. The objective is to ensure that IS personnel and others who may be involved in the planning process, are aware of the types of information that should be included in such plans; to provided a recommended structure and a suggested format; and generally to make those persons responsible aware of the criticality of the contingency planning process.

Federal Information Processing Standard on Trusted Systems Technology, Minimum Security Functionality Requirements for Multi-User Operating Systems, Issue 1, 16 January 1992.

This document provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems.

Federal Information Processing Standard on Trusted Systems Technology, Federal Criteria for Information Technology Security, Protection Profile Development, Volume 1, Version 1.0, December 1992.

This document provides a basis for developing, analyzing, and registering criteria for information technology (IT) product security development and evaluation. It explains how to use provided generic requirements as building blocks to create unique sets of IT product security criteria called protection profiles. There are four principal objectives:

- Develop an extensible and flexible framework for defining new requirements for IT product security
- Enhance existing IT product security development and evaluation criteria, 3) Facilitate international harmonization of IT product security development and evaluation criteria
- Preserve the fundamental principles of IT product security.

National Security Telecommunications and Information Systems Security Committee

NTISSD 500, Information Systems Security (INFOSEC) Education, Training, and Awareness, 25 February 1993.

This document establishes the requirement for federal departments and agencies to develop and/or implement Telecommunications and Automated Information Systems Security (TAISS) education and training programs and TAISS awareness activities.

NTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, 16 November 1992.

This document establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. For the purpose of the directive, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each phase of the life cycle.

NTISSD 502, National Security Telecommunications and Automated Information Systems Security, 5 February 1993.

This document delineates and clarifies objectives, policies, procedures, standards , and terminology as set forth in the "National Policy for the Security of National Security Telecommunications and Information Systems," (National Security Decision 42) dated July 1990.

The National Security Decision 42 establishes the initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding, from exploitation, systems that process or communicate national security information, and establishes a mechanism for policy development, and assigns responsibilities for implementation.

NTISSP 4, National Policy on Electronic Keying, 16 November 1992.

This document declares that all U.S. Government departments and agencies shall establish and implement electronic keying programs with the objective of virtually eliminating, by 2000, their dependence on paper-based/non electronic keying methods and with a goal of implementing benign keying where appropriate. Electronic keying shall be applied to all cryptographic processes related to national security systems. U.S. Government departments and agencies shall exchange electronic keying information freely, coordinate programs, and participate in consolidated programs wherever possible.

NTISSP 200, National Policy on Controlled Access Protection, 15 July 1987.

This document states that all automated information systems that are accessed by more than one user, when those users do not have the same authorization to use all of the classified or sensitive unclassified information processed or maintained by the automated information system, shall provide automated Controlled Access Protection for all classified and sensitive unclassified information.

Office of Management and Budget

Office of Management and Budget Bulletin No. 90-08 , Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, July 1990.

This document provides guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. It provides instructions and format for the preparation of system security plans.

Office of Management and Budget Circular A-130 , Revised (Transmittal Memorandum No. 2), Management of Federal Information Resources, Executive Office of the President, July 1994.

This document establishes general policy for the management of Federal information resources. Included in this circular is policy for the security of Federal ISs. The circular establishes minimum controls for inclusion in INFOSEC programs and assigns responsibilities for the security of ISs.

This document provides detailed interim guidance to Navy program managers on how to address computer security requirements during the acquisition process.

Naval Staff Office Publication 5239 Modules

Planned Naval Staff Office Publication 5239 Modules (Note: the modules are not listed in publication order. Modules that have been published are annotated as such.)

***5239-01 Introduction to Information Systems Security (INFOSEC)**

This document provides a basic introduction to INFOSEC and summaries the DoN INFOSEC Program.

***5239-02 Terms, Abbreviations, and Acronyms**

This document lists and defines INFOSEC terms, acronyms, and abbreviations that have been standardized for use within the DoN.

5239-03 Designated Approving Authority (DAA) Guidebook

This document provides guidance to the DAA in focusing the efforts of the activity security staff. Contains synopsis of certification and accreditation process. Offers the DAA a step-by-step approach to assist in reaching accreditation decisions.

***5239-04 Information Systems Security Manager Guidebook**

This document provides guidance to the individual assigned responsibility for INFOSEC implementation and operation at Navy activities . Illustrates the need for management involvement and support for the security program.

***5239-07 Information Systems Security Officer's Guidebook**

This document aids those who conduct and administer INFOSEC programs for specific ISs and Local Area Networks (LAN). Helps ISSOs understand the requirements, identify the necessary planning, and conduct an effective INFOSEC program.

***5239-08 Network Security Officer's Guidebook**

This document aids those who conduct and administer INFOSEC programs for specific networks and LANs. Helps Network Security Officers (NSO) understand the requirements, identify the necessary planning, and conduct an effective INFOSEC program.

***5239-10 Assessed Product List** (Published)

This document identifies products that have been evaluated for features and assurance of trust.

***5239-11 System Security Requirements Development**

This document provides guidance on how to develop a security policy and security requirements for a specific system.

5239-12 Acquisition Life Cycle Guidebook (PM/Developers)

This document identifies key technical and management actions need from Program Managers and other developers who have managerial and technical responsibilities for acquiring or certifying computer systems. Oriented

primarily towards Program Managers, it focuses on the processes and requirements needed to certify and accredit information systems.

***5239-13 Certification & Accreditation (C&A) Guidebook**

This document provides procedure guidance and decision aids for conducting C&A process activities to determine the suitability of a system to operate in a targeted operational environment based on the degree of assurance required and other factors related to a system.

5239-14 Security Architecture Guidebook

This document serves as a compendium of proven solutions to DON INFOSEC problems to assist INFOSEC systems engineering and customer support professionals to determine whether there are precedents for a customer's problem and to facilitate finding reusable solutions to common INFOSEC problems.

***5239-15 Controlled Access Protection Guide** (Published)

This document aids the user and security staff in understanding the DoN Controlled Access Protection policy, its relationship to C2, and techniques activities can use to acquire CAP-compliant systems.

***5239-16 Risk Assessment Guidebook**

This document provides policy and step-by-step procedures to individuals responsible for accomplishing a risk analysis on systems. Provides methods for the determination of system sensitivity and criticality, accomplishment of risk assessment and economic analysis, and determination of environmental hazards and threats to DoN information systems.

***5239-18 Security Test and Evaluation Guidebook**

This document provides information on how to perform security test and evaluation (ST&E) for information systems, embedded computers, and networks. It addresses microcomputers, minicomputers, mainframes, and specialized computers in both stand-alone and networked environments. The instruction provides general guidance and procedures to security managers and users for conducting ST&Es.

***5239-19 Computer Incident Response Guidebook**

This document aids the ISSM, ISSO, and users in responding to security incidents involving computer penetrations or malicious code. Provides general guidance for planning activity response and specific procedures for coordination with NAVCIRT.

5239-23 COMSEC Embedding Guidebook

This document provides design guidelines for embedding INFOSEC modules .

***5239-26 Remanence Security Guidebook** (Published)

This document provides policy, guidelines, and procedures for clearing and purging information systems memory and other storage media for release outside of and for reuse within controlled environments. It pertains to both classified and sensitive unclassified information. Implements DOD 5200.28-M and CSC-STD-005-85.

5239-29 Controls Over Copyrighted Computer Software (Published)

This document assists DON activities in developing and implementing their own policies and procedures for controlling and using computer software programs that have licensing agreements and copyright protection within the DON.